(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 564 825 A2**

# (12) EUROPEAN PATENT APPLICATION

(21) Application number: **93103555.4**

(51) Int. Cl.[5]: **H04L 9/00**, H04L 9/32

(22) Date of filing: **05.03.93**

(30) Priority: **11.03.92 FI 921055**

(43) Date of publication of application:
**13.10.93 Bulletin 93/41**

(84) Designated Contracting States:
**DE FR GB IT SE**

(71) Applicant: **NOKIA TECHNOLOGY GmbH**
**Östliche Karl-Friedrich-Strasse 132**
**D-75175 Pforzheim(DE)**

(72) Inventor: **Kangas, Mauri**
**Tallintie 2A10**
**SF-21530 Paimio(FI)**

## (54) Method for identification of secret data messages in a uni-directional multipoint network using cyclic redundancy checks.

(57) Invention relates to a method for identifying secret data messages in a one-direction multipoint network. The identifying of the data messages is carried out with the help of identification used for the error check. With the help of invention it can be identified to whom a message is meant without opening the secret data messages.

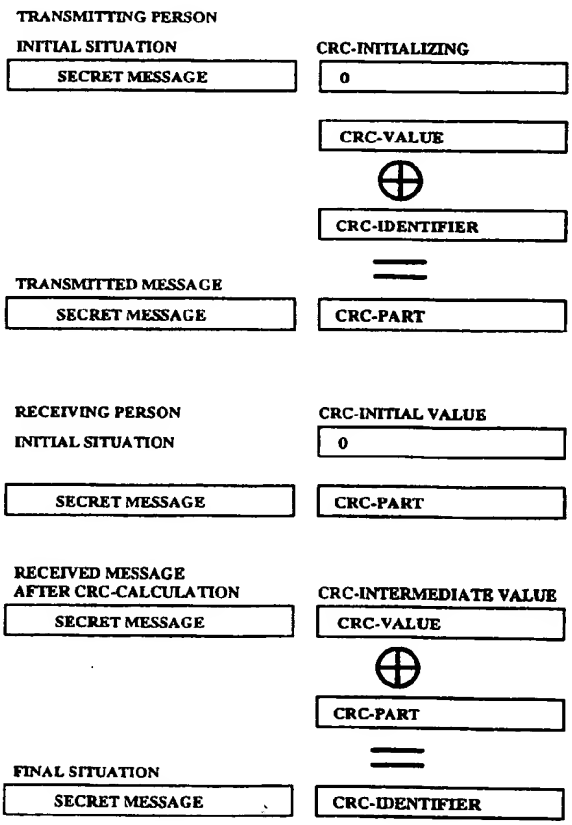


**Fig. 1**



EP 0 564 825 A2

This invention relates to a method for identifying secret data messages in a transmitting system where a cyclic redundancy code (CRC) or checksum is used for error check. With the help of the method according to the invention it can be identified to whom or to which group a message is potentially transmitted without increasing the amount of bits in the information transmitted and without opening all the secret data messages.

In a one-direction multipoint network unique messages are to be sent to several different receiving persons as a steady flow. The messages have been coded with a complicated algorithm which also involves error check. The lenght of the messages is to be kept as low as possible and the personalities of the receiving persons secret.

Since the messages cannot include the identification of the receiving person in a clear form, this must be included in the secret message. Because the receiving person to distinguish which ones of the messages are for him/her, all the receiving persons have to read all the messages. This takes too much time. It must be noted here that the messages can be personally coded so that the contents of a message meant for another receiving person cannot be solved. With the help of a personal identification receiving person can, after opening the message, determine whether the message was meant for him/her or not.

The background of the invention was to accomplish a transmitting system for secret data messages, where all the receiving persons would not have to read all the messages and where all the above mentioned problems can be solved. The purpose of the invention was then to accomplish a method for identifying to whom a message is potentially transmitted without increasing the amount of bits in the information transmitted and without opening all the secret data messages.

According to the first aspect of the present invention there is provided a method for identifying secret data messages in a transmitting system where a cyclic redundancy code (CRC) or checksum is used for error check, wherein the identifying of the data messages is carried out with the help of identification used for the error check.

Since all the messages have error check, such as a 16-bit CRC-code, this can be used in identifying the messages without increasing the length of the messages.

An embodiment of the present invention will now be described with reference to the accompanying drawings in which:

Figure 1 is a diagram illustrating transmitting and receiving of a secret message in the present invention.

Figure 2 is a diagram illustrating a coding circuit of a (n-k)-step transfer register according to the present invention.

Figure 3 is a diagram illustrating a decoding circuit of a (n-k)-step transfer register according to the present invention.

The diagram shown in figure 1 is a diagram of transmitting and receiving of a secret message in the present invention. In addition to the own personal identification each receiving person or group is given a unique CRC-identification which is used in transmitting end for CRC-calculation.

The diagram shown in figure 2 is a diagram of a coding circuit of a (n-k)-step transfer register according to the present invention. For the CRC-calculation of the secret message a back coupled transfer register is used which is initialized to "0" in CRC-calculation. When the CRC-value is calculated for the transmitted message, a 16-bit CRC-value is got with a 16-bit coding circuit. The CRC-value is taken to XOR-function together with the unique CRC-identification. The produced 16-bit CRC-part is added to the end of the message and transmitted to the receiver.

The switch is in position A during the secret message and in position B during the CRC-part. Instead of XOR-function there can be another function used, which can be reversed in the receiving end. Here XOR-function is taken as an example, since it very easy to realize in hardware CRC-calculation.

The diagram shown in figure 3 is a diagram of a decoding circuit of a (n-k)-step transfer register according to the present invention. The transfer register of the receiver is initialized to "0". When the secret message is now taken to the CRC transfer register of the receiver, the last state of the transfer register will now have the CRC-value of the receiving person, if the appropriate message is meant for the receiving person and error-free. The switch positions correspond to the figure 2.

If there is an error in transmitting, the receiving persons might have misinterpretations as to whom the message is meant. If the amount of errors stays low, the receiving persons do not need to open the messages unnecessarily.

When there is a lot more receiving persons than implied by the CRC-identification (if the CRC-value is 16 bits, the CRC-identification can be for example 16, 7 or 6 bits) several receiving persons need to have the same CRC-identification. Because of this a lot of messages are opened unnecessarily. Because the messages always contain the identification of the receiving person, the receiving persons do not get wrong information.

The error check value can be so long that it includes both error check and data message identification, but it does not necessarily need to be. If the error check parts are taken along, the XOR-operation is only carried out with a part of the

check part bytes or the check part is totally different. If the XOR-operation is carried out with the whole error check value and the error check is so left out, the method used however includes an error check as after opening an unique message the receiving persons own address must be found inside the opened message.

## Claims

1. A method for identifying secret data messages in a transmitting system where a cyclic redundancy code (CRC) or checksum is used for error check, wherein the identifying of the data messages is carried out with the help of identification used for the error check.

2. A method as claimed in claim 1, wherein in addition to the own personal identification each receiving person is given a unique CRC-identification, which is used in transmitting end for CRC-calculation.

3. A method as claimed in claim 2, wherein the calculated CRC-value, together with the unique CRC-identification, is performed such function that can be calculated reversely in the receiving end, the result value is added to the end of the secret data message and is sent to the receiver.

4. A method as claimed in claim 3, wherein the calculated CRC-value, together with the received CRC-part, is performed the corresponding reverse function in the receiving end, which gives the CRC-identification of the receiving person in question as a result, when the message is meant for the receiving person in question.

5. A method as claimed in claim 3 or 4, wherein the function performed to the CRC-value is so called XOR-function.

6. A method as claimed in any of the preceding claims, wherein checksum is used instead of the CRC-value.

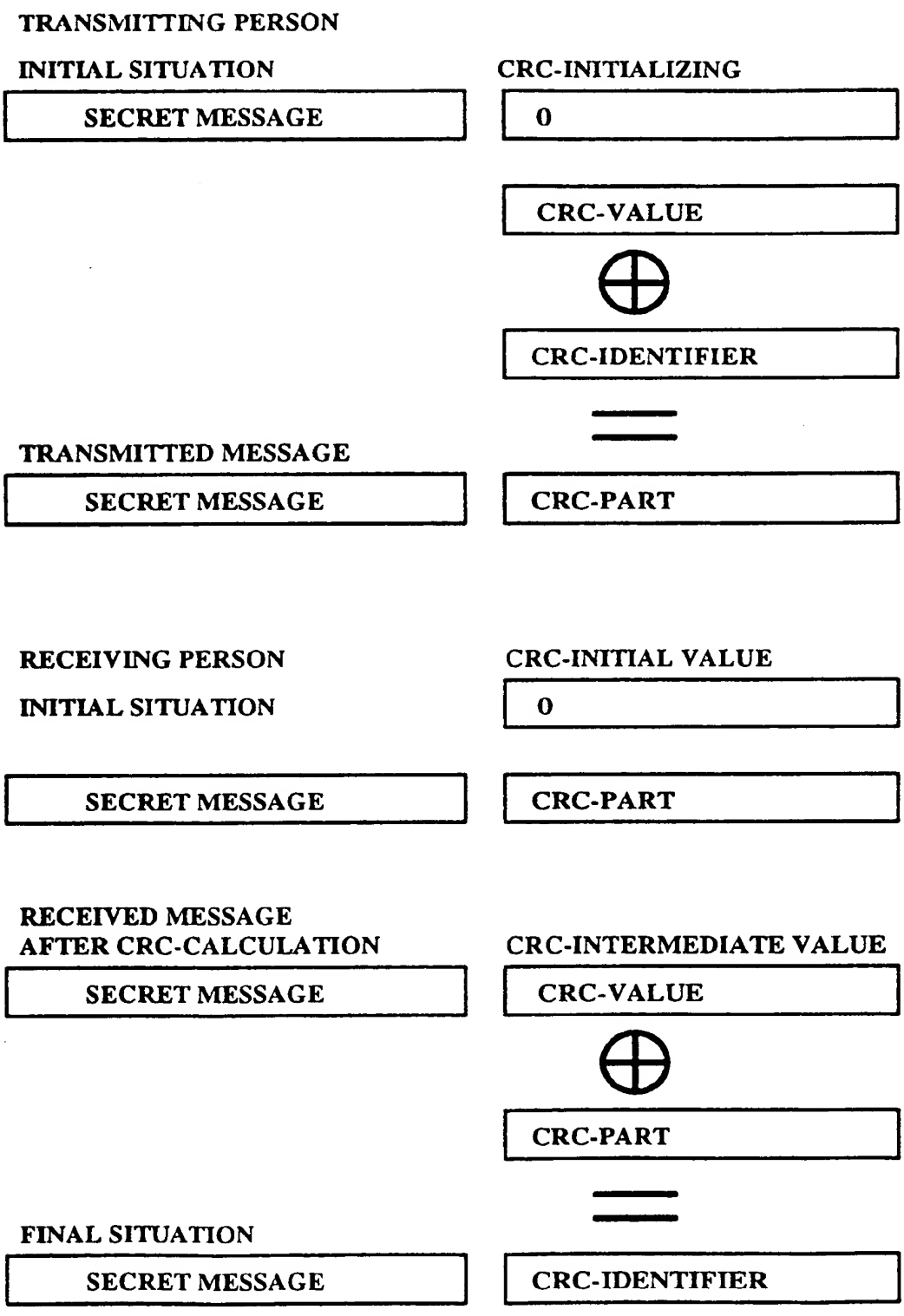
TRANSMITTING PERSON
INITIAL SITUATION
CRC-INITIALIZING
SECRET MESSAGE
0
CRC-VALUE
CRC-IDENTIFIER
TRANSMITTED MESSAGE
SECRET MESSAGE
CRC-PART
RECEIVING PERSON
INITIAL SITUATION
CRC-INITIAL VALUE
0
SECRET MESSAGE
CRC-PART
RECEIVED MESSAGE
AFTER CRC-CALCULATION
CRC-INTERMEDIATE VALUE
SECRET MESSAGE
CRC-VALUE
CRC-PART
FINAL SITUATION
SECRET MESSAGE
CRC-IDENTIFIER

**Fig. 1**

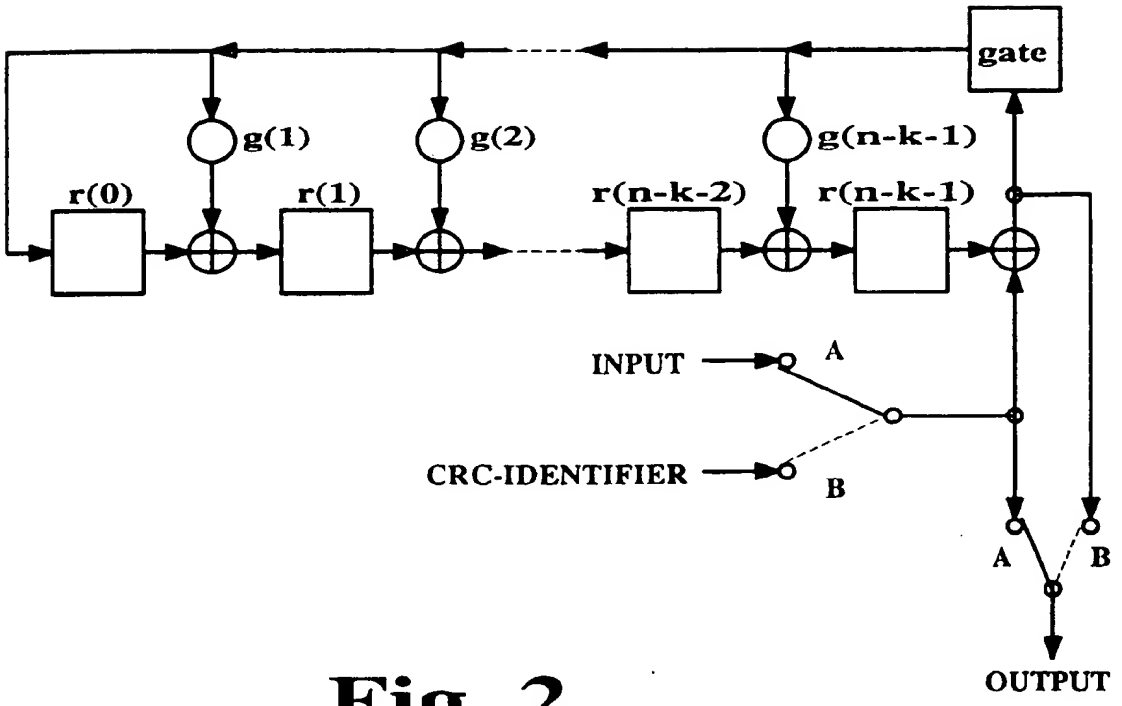
gate
g(1)
g(2)
g(n-k-1)
r(0)
r(1)
r(n-k-2)
r(n-k-1)
INPUT
A
CRC-IDENTIFIER
B
A
B
OUTPUT

Fig. 2

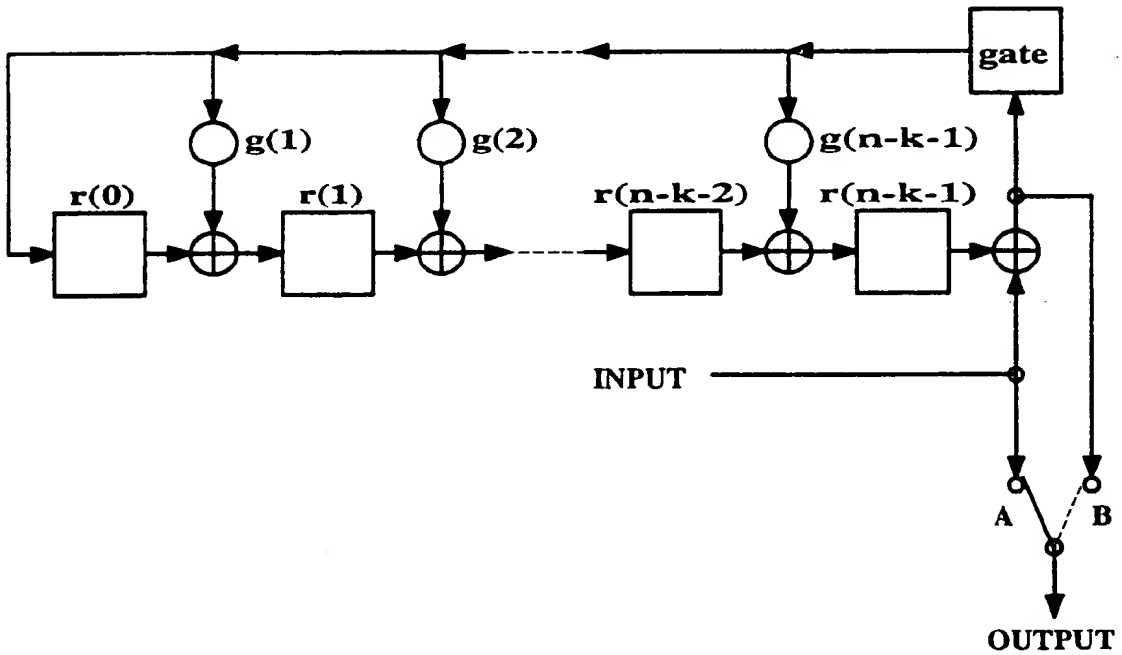
gate
g(1)
g(2)
g(n-k-1)
r(0)
r(1)
r(n-k-2)
r(n-k-1)
INPUT
A
B
OUTPUT

Fig. 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 564 825 A3**

# (12) EUROPEAN PATENT APPLICATION

(21) Application number: **93103555.4**

(51) Int. Cl.[6]: **H04L 9/00**, H04L 9/32

(22) Date of filing: **05.03.93**

(30) Priority: **11.03.92 FI 921055**

(43) Date of publication of application:
**13.10.93 Bulletin 93/41**

(84) Designated Contracting States:
**DE FR GB IT SE**

(88) Date of deferred publication of the search report:
**03.05.95 Bulletin 95/18**

(71) Applicant: **NOKIA TECHNOLOGY GmbH**
**Östliche Karl-Friedrich-Strasse 132**
**D-75175 Pforzheim (DE)**

(72) Inventor: **Kangas, Mauri**
**Tallintie 2A10**
**SF-21530 Paimio (FI)**

## (54) Method for identification of secret data messages in a uni-directional multipoint network using cyclic redundancy checks.

(57) The invention describes a method for identifying the intended recipients of secret data messages in an unidirectional multipoint network where a cyclic redundancy code (CRC) or checksum is used for error checking. Once a CRC-value has been calculated for the message to be transmitted, it is XOR-ed with a CRC-identification number which is unique to each receiver or group of receivers, and the result is transmitted. Only the intended receiver will then be able to decode the CRC-value from the combined value in order to process the message correctly.

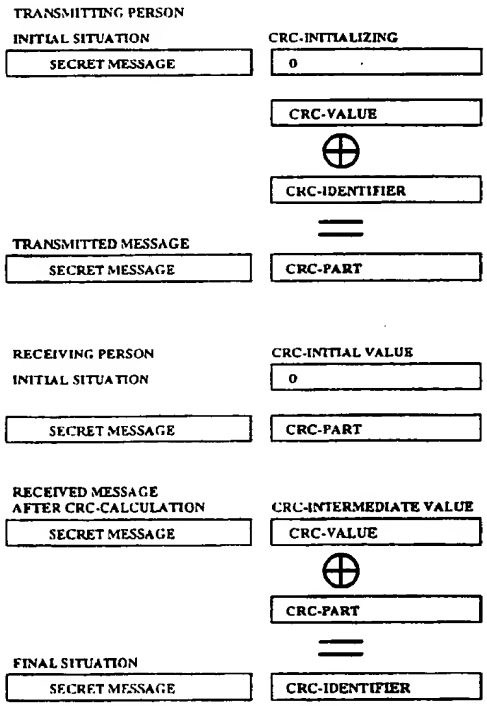


**Fig. 1**

EP 0 564 825 A3

European Patent Office

# EUROPEAN SEARCH REPORT

Application Number
EP 93 10 3555

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int.Cl.5) |
|---|---|---|---|
| X | US-A-4 771 458 (CITTA ET AL.)<br>* column 1, line 60 - column 3, line 6 *<br>* column 4, line 4 - line 33 *<br>* column 4, line 43 - column 6, line 20 *<br>* column 7, line 17 - line 19 *<br>* figures 1-3 * | 1 | H04L9/00<br>H04L9/32 |
| A | IEEE TRANSACTIONS ON COMMUNICATION TECHNOLOGY,<br>vol.COM-17, no.1, February 1969, NEW YORK US<br>pages 42 - 48<br>D.MANDELBAUM 'AN APPLICATION OF CYCLIC CODING TO MESSAGE IDENTIFICATION'<br>* page 42, right column, line 1 - page 44, left column, line 15 * | 1 | |

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

H04L

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| THE HAGUE | 28 February 1995 | Lydon, M |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1500 03.82 (P04C01)

# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [ ] FADED TEXT OR DRAWING
- [ ] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [x] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

**IMAGES ARE BEST AVAILABLE COPY.**
**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**